International Journal of Advanced Social Sciences and Education (IJASSE)
Vol. 3, No. 5, 2025: 335-350

Who Dem Be: Profiling the Yahoo Boys in Metropolitan Lagos

Isimenmen Akhimien[1], Adedeji Oyenuga[2]*, Olanrewaju Ajiboye[3]
Department of Sociology, Madonna University, Nigeria
Corresponding Author: Adedeji Oyenuga adedeji.oyenuga@lasu.edu.ng

A R T I C L E I N F O

Keywords: Cybercrime, Youths, Lagos State, Space Transition Theory, Yahoo-Boys, Socio-Demographic, Nigeria

Received:19, August
Revised: 20, September
Accepted: 30, October

A B S T R A C T

The increasing involvement of young people in cybercrime in Nigeria has become a major concern for scholars, policymakers, and security institutions. This paper examines the features of young cybercrime offenders in Lagos State with a view to understanding their socio-demographic and psycho-demographic characteristics. Employing a mixed-method approach, data were collected through structured questionnaires administered to 277 convicted cybercrime offenders and 20 key informant interviews with law enforcement agents. Drawing on both quantitative and qualitative data obtained from correctional centres and key informant interviews (KIIs) with law enforcement agents, the study found that most offenders are male youths between 18 and 29 years, predominantly from the southern part of Nigeria. Psycho-demographically, they exhibit traits such as lavish spending, substance use, low empathy, and a quest for quick wealth. The paper employs Space Transition Theory to explain how anonymity in cyberspace allows offenders to drift from conformity in physical space to deviant behavior online. The findings provide insight into the evolving identity, motivations, and social organization of young cybercrime offenders, offering policy implications for intervention and rehabilitation.

DOI: https://doi.org/10.59890/ijasse.v3i5.179
ISSN-E: 2988-2133
https://dmimultitechpublisher.my.id/index.php/ijasse

INTRODUCTION

Cybercrime among youths in Nigeria has emerged as a pressing socio-economic and security challenge. Over the last two decades, the rise of internet access, mobile technologies, and online financial platforms has provided fertile ground for fraudulent activities, popularly known as "Yahoo-Yahoo" scams. These activities are primarily undertaken by young males aged 18–29, often with at least secondary school education, who exploit digital anonymity to pursue rapid financial gain (Adeniran, 2008; Osho & Eneche, 2019).

The prevalence of youth cybercrime in Nigeria reflects a complex interplay of structural, socio-cultural, and technological factors. High levels of unemployment, economic instability, and limited access to legitimate economic opportunities create conditions that render illegal online ventures appealing. Lazarus (2018) notes that societal glorification of wealth, particularly in popular culture and media, reinforces the notion that financial success (regardless of the source) commands respect and social status. This normalization has cultivated a subculture among Nigerian youths where cybercrime is framed as an entrepreneurial pursuit rather than a criminal act.

Internet penetration in Nigeria has expanded rapidly, particularly in urban centers like Lagos State, which hosts a heterogeneous youth population and a dense network of cybercafés. Sanou (2017) reports that over 80% of youths globally are active internet users, with Nigeria among the top countries for online youth engagement. Within this context, Lagos State presents a microcosm of the broader societal and technological trends facilitating youth involvement in cybercrime. The internet, while fostering education, social interaction, and entrepreneurship, simultaneously provides opportunities for deviant behavior due to its perceived anonymity and the difficulty of law enforcement monitoring (Katz & Rice, 2003; Borgmann, 2004).

From a sociological perspective, cybercrime represents a digital adaptation of socio-economic pressures. Lin (2001) and Katz and Rice (2002) argue that new media technologies both reinforce and challenge existing social inequalities. Youths facing economic deprivation or social marginalization may rationalize online fraud as a legitimate strategy for upward mobility. Similarly, Nguyen and Western (2007, cited in Oyenuga, 2017) suggest that the digital divide has narrowed, providing widespread access to information and tools, but this has also blurred moral boundaries for vulnerable populations.

Prior research categorizes the consequences of internet use into behavioral, social, economic, legal, and psychological dimensions (Kukar-Kinney, Intihar, & Leahy, 2008). Many of these dimensions intersect with cybercrime motivations, highlighting that youth online deviance is not solely about financial gain but is also influenced by social recognition, identity formation, and the desire for status within peer networks. Cyber offenders often perceive internet fraud as low-risk yet highly rewarding, reflecting a moral detachment and calculated risk-taking behavior (McAfee Reports, 2007).

In light of these factors, this study focuses on Lagos State to examine the socio-demographic and psycho-demographic characteristics of young cybercrime offenders. By investigating who these offenders are, how they

operate, and the psychological and social mechanisms that underpin their actions, the research seeks to provide a nuanced understanding of youth involvement in cybercrime. Specifically, the study aims to identify the socio-demographic features of these offenders, including age, education, and family background, while also examining the psycho-demographic traits that distinguish them from law-abiding peers. Additionally, the study explores the influence of social networks, peer dynamics, and cultural norms on online deviance, highlighting how environmental and interpersonal factors facilitate engagement in cybercrime. By integrating theoretical perspectives with empirical findings, the research also seeks to generate actionable insights for policy formulation, prevention, and rehabilitation strategies, contributing to broader academic discourse on youth cybercrime in Nigeria.

LITERATURE REVIEW

Space Transition Theory

The study adopts Jaishankar's (2008) Space Transition Theory, which explains how individuals move between physical and virtual spaces, exhibiting different behavioral patterns. According to this theory, persons with repressed criminal tendencies in physical space may commit crimes in cyberspace where anonymity and identity flexibility offer freedom from social constraints. Key tenets of Space Transition Theory include:

1. Repressed Deviance: Individuals with latent criminal tendencies in the physical world may express these in cyberspace, where perceived anonymity mitigates fear of reprisal.
2. Identity Flexibility: Online environments allow offenders to maintain dual identities—law-abiding in physical society while engaging in deviant acts online.
3. Collaborative Networks: Offenders often operate in organized teams, with distinct roles (catchers, pickers, sitters), enabling complex fraud schemes that are difficult to dismantle without coordinated enforcement efforts.

This theory is particularly relevant for understanding Nigerian youths engaged in cybercrime. KIIs conducted in this study revealed that older "mentors" often guide younger offenders, illustrating the transfer of knowledge and reinforcement of deviant norms within online social networks. These networks facilitate not only the technical execution of cyber fraud but also the social normalization of these behaviors, consistent with the theory's assertion that cyberspace provides an enabling environment for the expression of repressed tendencies.

Space Transition Theory also accounts for contextual and socio-cultural dimensions. For example, in Lagos State, cyber offenders often justify fraudulent activities as legitimate "hustle" work, reflecting societal narratives that valorize wealth accumulation. By integrating this theoretical lens with socio-demographic and psycho-demographic analysis, the study elucidates not only who these offenders are, but also why cyberspace enables their deviance.

METHODOLOGY

This study adopted a mixed-methods research design, combining quantitative surveys with qualitative Key Informant Interviews (KIIs), to provide a robust and comprehensive understanding of youth cybercrime in Lagos State. The mixed-methods approach is particularly suited for research on cybercrime, as it allows for the collection of both measurable data on socio-demographic and psycho-demographic traits and rich qualitative insights into behavioral patterns, motivations, and organizational structures. Such an approach facilitates triangulation, enabling the researcher to validate findings across multiple sources and enhance both the reliability and credibility of the study (Creswell, 2014; Johnson & Onwuegbuzie, 2004). By integrating quantitative and qualitative methodologies, the study was able to examine not only who the offenders are, but also how and why they engage in cybercrime within their social and technological environments.

The study population consisted of two distinct but complementary groups: young cybercrime offenders incarcerated in Lagos State correctional facilities and law enforcement personnel directly involved in cybercrime investigation and prosecution. The offender group included male youths predominantly aged between 18 and 35 years, as previous studies have identified this cohort as the most active in online fraudulent activities (Adeniran, 2008; Tade & Aliyu, 2011). Female offenders, though significantly fewer in number, were also included to ensure a representative understanding of youth cybercrime. Law enforcement participants comprised officers from the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force, particularly those assigned to cybercrime units. Their inclusion provided expert perspectives on offender behavior, organizational networks, and enforcement challenges, which complemented the self-reported data from offenders.

A total of 277 convicted cybercrime offenders were purposively selected from five correctional facilities in Lagos State: Ikoyi Medium, Kirikiri Medium, Kirikiri Maximum, Kirikiri Female, and Badagry Medium Security Custodial Centres. These facilities were strategically chosen for their high concentration of cybercrime offenders and their accessibility for research purposes. The purposive sampling method allowed the researcher to target participants who had direct experience with cybercrime offenses, ensuring the collection of relevant and meaningful data. Additionally, 20 Key Informant Interviews were conducted with law enforcement officers. Participants were purposively selected based on their experience, years of service, and direct involvement in investigating or prosecuting cybercrime cases, which ensured the credibility and depth of the qualitative insights collected.

Data were collected using two primary instruments. The quantitative instrument was a structured questionnaire designed to gather detailed information on socio-demographic characteristics, psycho-demographic traits, and behavioral patterns of offenders. The questionnaire included multiple-choice questions, Likert-scale items, and closed-ended questions covering variables such as age, gender, education, spending habits, online activity,

substance use, and social networks. This instrument was chosen for its ability to capture standardized data across a large sample, facilitating statistical analysis and comparison. The qualitative instrument consisted of a semi-structured interview guide for KIIs, which provided flexibility for respondents to elaborate on their experiences and observations. This guide allowed law enforcement officers to discuss offender behavior, organizational hierarchies, recruitment patterns, and other nuanced aspects of cybercrime that are difficult to quantify.

Data collection was carried out over three months and involved careful coordination with correctional facility administrators and law enforcement agencies. Inmates completed the structured questionnaires under supervision, ensuring the accuracy and completeness of responses while maintaining their autonomy. KIIs were conducted in secure offices or via telephone interviews, depending on the availability and preference of participants. Each interview lasted between 45 and 60 minutes, and all were audio-recorded with informed consent before being transcribed for analysis. The researcher maintained a non-judgmental stance throughout data collection, which helped establish trust and encouraged participants to provide candid responses.

Ethical considerations were central to the study design. Participation was voluntary, and all respondents were informed of their right to withdraw at any stage without any negative consequences. Respondents were assured of the confidentiality of their responses, and personal identifiers were not collected in the surveys. KII transcripts were anonymized using coded identifiers, and all data were securely stored to prevent unauthorized access. The study also took into account the power dynamics inherent in researching incarcerated populations, taking steps to minimize coercion and ensure that participants felt comfortable and respected. Ethical approval was obtained from relevant institutional and correctional authorities, reflecting adherence to established standards for human subject research.

Quantitative data were analyzed using descriptive statistics, including frequencies, percentages, and cross-tabulations. These techniques enabled the researcher to summarize the socio-demographic and psycho-demographic characteristics of offenders and identify patterns across different variables. Results were presented in tables and charts to enhance clarity and facilitate interpretation. Qualitative data from KIIs were analyzed thematically, with transcripts coded to identify recurring patterns, concepts, and insights regarding offender behavior, social organization, and motivational factors. Themes were iteratively refined through constant comparison and reflection, allowing the researcher to draw nuanced conclusions about the nature and dynamics of youth cybercrime in Lagos State. The integration of quantitative and qualitative data provided a multidimensional perspective, reinforcing the validity of the study findings.

The study focused exclusively on Lagos State, a major commercial and technological hub in Nigeria, to capture the complex interplay of urban, economic, and digital factors influencing cybercrime. While this focus enhances contextual depth, it limits the generalizability of the findings to other regions or international settings. Furthermore, reliance on self-reported data introduces

the potential for social desirability bias, although the assurances of anonymity and confidentiality were intended to mitigate this effect. Despite these limitations, the methodology provided a comprehensive framework for understanding the characteristics, motivations, and organizational structures of young cybercrime offenders, producing findings that are both empirically grounded and analytically robust.

RESULT AND DISCUSSION

Socio-Demographic Characteristics of Respondents

Table 1. Socio-Demographic Characteristics of Young Persons Involved in Cybercrime

Variable		Frequency (277)	Percentage (100)
Age	Lowest through 15	74	29.2
	16-20	130	51.4
	21- 25	46	18.2
	Highest through 26	3	1.2
	Total	**253**	
Gender			
Female	Yes	80	30
	No	187	70
	Total	**267**	
Male	Yes	277	100
	No	0	
	Total	**277**	

Source: Field Survey

The table above presents the age distribution of young persons involved in cybercrime. A little above half of the respondents (51.4%) opined that individuals involved in cybercrime are usually between the ages of 16 and 20 years. About a quarter of the respondents (29.2%) opined that cybercrime offenders can be found from 15 years and below. A few of the respondents (18.2%) opined that cybercrime offenders are between the ages of 21 and 25 years old. An insignificant few (1.2%) opined that people involved in cybercrime are above 26 years.

This corresponds with the findings in the Key Informant Interviewees, who opined that the age at which cybercrime offenders begin is usually at the age of 13. One of the respondents stated that *"...they can be found from age 14-40…"* (KII/RES9/2023)

Another opined that *"…presently we start seeing from 13 years upward…"* (KII/RES1/2023). A law enforcement officer opined that

> …they are usually below 18, i.e, (16-23). Those who are over 30 years are generally masters and retired, and they serve as mentors and trainers for the young ones… (KII/RES10/2023)

The table above also shows the gender distribution of young people involved in cybercrime. All the respondents (100%) opined that individuals involved in cybercrime are male, while less than half of the respondents (30%) opined that females are involved in cybercrime.

This correlates with the response from a respondent who opined that "*…yes, you have females that do fraud…"* (KII/RES3/2023).

Another respondent stated emphatically that "*…90% are men and women are usually involved in relationships..."* (KII/RES11/2023).

A third respondent opined that "*more ladies are involved in cybercrime…. females also do Yahoo…*" (KII/RES7/2023).

A respondent, when asked the area of the country where cybercrime is more prevalent, opined that "*…yes, south-west, south-east and south-south. That means that they are mostly populated in the southern part of the country…"* (KII/RES2/2023). Another respondent stated in correlation to the first statement that "*…they are not even in the north...*" (KII/RES3/2023). Furthermore, one of the respondents was very specific about areas with the highest concentration of cybercrime offenders, he stated that "*…Ekpoma, Benin, Auchi have the highest concentration of yahoo-boys…* (KII/RES7/2023)*"*

When the key informants were asked about the average educational level of cybercrime offenders, one of the respondents opined that

> "…there are some that are very uneducated, such as SSCE holders or dropouts. Their educational level does not matter; some of them are very brilliant university students, and you will also see some of them who are secondary school dropouts… (KII/RES12/2023)

Aside from the socio-demographic characteristics of cybercrime offenders in Lagos state, many other attributes were identified by the study, such as mode of dressing, favourite hangouts, physiological traits, and manners of address within and outside the group. The table overleaf shows characteristics of cybercrime offenders.

Psycho-Demographic Characteristics of Young People Involved in Cybercrime

Table 2. Psycho-Demographic Characteristics of Young People Involved in Cybercrime

Variable		**Frequency (277)**	**Percentage (100%)**
Street smarts	Yes No Total	80 176 256	31.3 68.8
Womanizing	Yes No Total	199 57 256	77.7 22.3
Substance abuse	Yes No Total	199 57 256	77.7 22.3

Sunk in eyes	Yes No Total	43 213 256	16.8 83.2
Tech savvy/ Education	Yes No Total	82 174 256	32 68
Lavish Spending/ Noisy/ Rude	Yes No Total	204 52 256	79.7 20.7
Opportunistic/ Manipulative	Yes No Total	159 97 256	62.1 37.9
Lack of Empathy	Yes No Total	199 57 256	77.7 22.3
Quest for Quick Wealth	Yes No Total	199 57 256	77.7 22.3
Online Anonymity/Presence	Yes No Total	203 53 256	79.3 20.7
Spiritual	Yes No Total	99 157 256	38.7 61.3
Attractiveness/ Self Confidence	Yes No Total	206 50 256	61.3 38.7

Source: Fieldwork, 2023

The table above shows that the major characteristic of cybercrime offenders in Lagos is that they are lavish spenders, noisy and rude (79.7%). This is consistent with the responses from the key informant, one of which opined that

> *…First and foremost, they are very rude. They do not have regard for anybody. For the fact that he has money, he does not have regard for anybody. A normal yahoo boy looks at a salary earner as if he is not working. You know that in Nigeria, it is not easy for a person to be earning one million naira monthly and this is something that a yahoo-boy can earn in one day. So, he does not have regard for anybody, they do not have respect… (KII/RES2/2023)*

Another respondent asserted that:

> *…because of their extravagant lifestyle... They are mannerless and uncultured, they talk to people anyhow especially when they are in restaurants. Go to club houses, you will see all these yahoo-boys there. they can spend 3million or 2 million without blinking…(KII/RES7/2023)*

A third law enforcement agent expatiated on the level at which they spend extravagantly with an example. He said

> *…Just imagine one yahoo boy came one day and said that he cannot do salary work because there is not any that can take him for the whole month. He said that his spending for a day was at least 500,000 Naira. that is about 15 million naira every month. And once he buys a new I phone, he is just counting down to buy another one and you as a salary earner cannot do such. If you do not have the heart, they will just put pressure on you. You will see him coming with a vehicle of 40 something million, after a month, he will change it to another one. He will tell you say he went and bought 80 million... (KII/RES15/2023)*

The table also shows that another major feature of cybercrime offenders is online anonymity and presence (79.3%). It further shows that the lack of empathy, low level of morality, quest for quick wealth, womanizing and substance abuse are other important characteristics of cybercrime offenders (77.7%).

This is consistent with the findings in the qualitative research which found that there was a significant association between cybercrime and substance abuse. One of the law enforcement officers said that *"…an average yahoo-boy is rude and a drug addict…"* (KII/RES3/2023).

Another respondent further explained that *"…they also indulge themselves in hard drugs because they now have the money to buy them…"* (KII/RES1/2023).

A third respondent on substance abuse explained why it is significantly related with cybercrime. He noted that *"…drugs make them to stay awake because of their clients time zones..."* (KII/RES16/2023). Lack of empathy is also consistent with the qualitative data as a respondent stated that

> *…No criminal has empathy. Empathy is different from sympathy o. It means being able to put yourself in another person's shoes. why would I put myself in the shoes of someone I want to de-fraud. I don't care about the person. The individual can go to hell… (KII/RES1/2023)*

Another law enforcement agent opined that

> *They are very wasteful and spend a lot of money on expensive things. They are usually very popular in clubs because they spend a lot of money. They also womanise. Drinking and smoking is also where they spend a lot of their money. (KII/RES8/2023)*

A third respondent further explained that

> *…another thing you need to note is that, this drug they take is to keep them awake. To make them functional in communication to send message at a particular time the client must have given an appointment. They understand that for you to succeed with a client, the client has to talk to you in his own time and whenever the appointment is not kept, it means the client is gone… (KII/RES20/2023)*

The study also found that they are usually seen walking in groups. This is because of the sensitive nature of their job; they do not like to mingle with

people that are not also involved in the business. One of the law enforcement agents opined that there needed to be at least three people for a successful venture. He opined that

> *…that goes back to where we say they are always in groups, everyone has a vital role to play in the game. In the game they have a catcher, a picker, a sitter. A sitter is the person who always purifies the business and makes it to be perfect. When a catcher gets the victim, it is the sitter that speaks with the victim and convince the victim that the whole thing is real. The sitter is always having conversation with the victim until he or she falls. Once money comes in, the picker goes to pull out the money back home where everybody shares. (KII/RES14/2023)*

He further opined that there is also usually the presence of a hacker. He stated that

> *…the picker is also a hacker. He goes in search of information in white systems, he checks, interacts from chats, from details you may have given, he now pushes to whom will be able to talk with you in terms of what you want to hear. As they work together, some have more experience in these practice than the others, you may be very good in interacting with clients, you may be very good in bringing clients for them to defraud. (KII/RES14/2023)*

The use of nicknames to change their identity was another characteristic that the study found. They mostly use these nicknames to avoid detection and to further remove themselves from the crime. They are very flashy people who like to show off their ill-gotten wealth. They are known to be very extravagant when they have parties or a reason to celebrate which could be a birthday celebration for both themselves and their girlfriends or just the success of a high paying scam.

To buttress the above point, an enforcement agent reiterated that:

> *…Most of them banish their real names to the unconscious to further hide their identities. Like for instance here, they use names like 'don' and 'parole' and so many other names. Within their circle, they also use slangs that a third party may never decode, and they have names for so many things and people. For example, a laptop is called 'lapi' or 'igba aje' and they call their victims' names like 'mayi', 'maga' or 'mugun'. (KII/RES20/2023)*

The study also found that there is a relationship between cybercrime and cultism. To this vein, one of the law enforcement agents opined that:

> *You see the cultism comes in whereby the money is dropping through a particular person and the person is not ready to remit the money. They call that kind of person a ripper. And if this person is a cultist, he believes that you both know that you do not have anything. That kind of person will always want to do anyhow but if the other person is a cultist as well, he will have his own people and they will start chasing each other… You know this yahoo, I cannot stand on my own, it is always a syndicate. If I am*

> *to push the money now, and I am in aye [fraternity], and you are not doing in it before or you are not a member of any cult (just a free person). When you want me to finish the job for you, and you want me to do it perfectly, come and join my cult. You are sure of the money and you will go for the initiation. Automatically, you have become a cultist. (KII/RES10/2023)*

Another respondent on cultism argued that *"…this individual was arrested for cultism o. It was when I wanted to search his phone and he refused and then confessed that he was a yahoo-boy…"* (KII/RES16/2023).

Other attributes identified by the study include: street smarts (31.3%); sunk in eyes (16.8%); technological know-how and education (32%); attractiveness and self-confidence (61.3%).

> *You cannot recognize them by just looking at them. Some are dressed more corporate and responsible. Wearing dreads makes one appear irresponsible to an extent. They may disguise in different forms. They are usually young people that have a lot of money but you cannot see how they are making their money; they also live expensive lives by buying expensive and flashy cars, phones, etc; they know how to operate expensive phones and computers; they work as a syndicate. They usually disguise as business men such as importer and exporters. (KII/RES11/2023)*

This is true, but it is too much of a coincidence for one individual to possess all these traits both physical and psychological at once.

A little above half of the respondents opined that individuals involved in cybercrime are usually between the ages of 16 and 20 years. About a quarter of the respondents opined that cybercrime offenders can be found from 15 years and below. A few of respondents opined that cybercrime offenders are between the ages 21 and 25 years old. A few opined that people involved in cybercrime are above 26 years. This finding is consistent with the findings of Rich (2018) who opined that cybercrime offenders are adolescents between the ages of 12 and 16 years. Although, the finding was inconsistent with the findings of Aransiola and Asindemade (2011) who reported that 50% of their respondents were between the ages of 22 and 25, while 40% were between the ages of 26 and 29. Aside from the age category, this study also found that cybercrime offenders are not just of the male gender, there are also females involved in cybercrime. The findings made from the qualitative study also echoed this point. The law enforcement agents opined that there were females involved in cybercrime and that the extent of their participation was usually determined by the script which was being acted out. The study also found that they are usually accomplices and not the main leader of the syndicate. This is consistent with the findings of Aransiola and Asindemade (2011) who opined that 5% of internet fraud offenders are females.

Another socio-demographic feature of cybercrime offenders that was found by the study was their educational level. The study found that cybercrime offenders can be found at all educational levels. The major percentage are SSCE holders, while a very few of them possesses either higher

or lower qualifications. Most of the law enforcement agents opined that there are educated and uneducated cybercrime offenders. They also opined that what is important with cybercrime offenders is the ability to read and write. They further opined that cybercrime offenders can be found even in as early as primary and secondary schools. The findings of this study was consistent with that of Adeniran (2008:349) who reported that "out-of-school due to distortions in school calendar and unemployed youths constitute a considerable percentage of the yahooboys in Nigeria". Although, it was inconsistent with the findings of Tade and Aliyu (2011) and Aransiola and Asindemade (2011) who opined that cybercrime offenders are usually university students and can be found in university environment.

The study also found that cybercrime offenders work in groups. Whitty (2018) argued that cybercrime offenders are usually found in gangs. She opined that the reason for that is because they fit the age group that are most likely to use the internet. As a result of the qualitative analysis, it was found that there needed to be a minimum of three individuals for a successful scam to play out. There needed to be a Picker, Catcher, and Sitter. The Catcher is usually the one that brings in the potential victim, while the Sitter is the individual that sits on the potential 'client', while making sure that the victim falls prey to their schemes. The Picker is the individual that goes to make sure that the money earned is successfully gotten from the victim and shared among themselves.

The study also found that cultism and substance abuse is a major characteristic of cybercrime offenders. One of the law enforcement agents opined that the wealth they get allow them the opportunity to be able to afford these substances. Another further expatiated their need for illegal substances as a way to keep them awake due to the differences in time-zone between them and their victims who may be in other continents. This is consistent with the findings of Babatunde (2012) who opined that cybercrime and other crimes such as prostitution, and violence are significantly associated with illicit drug abuse. Some law enforcement agents opined that cultism is a necessity for cybercrime offenders as it protects them from other cultists or individuals that might have the intention to rip them off of their money. In the cybercrime community, such an individual is called a "ripper".

A major feature of cybercrime offenders that was found by the study is that they usually try to disguise and be anonymous online (79.3%). This is in contrast to other features found by the study which are lavish spending and rudeness (79.7%); and womanizing (77.7%). Their flashy lifestyle is in contrast with their need for anonymity because it makes them easily detectable. A study conducted by Ojedokun and Eraye (2012) titled Socioeconomic lifestyles of the yahoo-boys: A study of the Perceptions of University Students in Nigeria interviewed students from three major Nigerian universities. More than half of the respondents of this study perceived the students engaged in cybercrime to be very extravagant. The authors of this study further opined that the wealth of cybercrime offenders was very temporary because of their flamboyant lifestyles. This shows that the need to brag and boast about their wealth overshadows the need for anonymity. It might be because most of them are from poor homes and

have the need to show everyone around them that they are wealthy, while damning the consequences. This finding is also consistent with one of the tenets of the space transition theory (Jainshankar, 2008) which states that:

Identity Flexibility, dissociative anonymity and the lack of deterrence factors in cyberspace provide the offenders with the choice to commit cybercrime. This is because they may use fake identities online which makes it easier for them to move from conformity (offline) to non-conformity (online). It allows them to live dual lives without the threat of exposure. Cybercrime offenders are very similar to every other person on the internet and the only difference is the 'intention" with which they are using the internet.

Another feature that was found by the study is the psychological makeup of a cybercrime offender. The study found that the lack of empathy, the quest for quick wealth, and manipulative tendencies were major attributes of cybercrime offenders. This is consistent with the findings of Lipsey & Chrystal (2007), who opined that there exists a large gap between the rich and the average, as such many strive to level up using the quickest means possible, since for any business to thrive well, the rate of return in the investment must be growing at a geometric rate with a minimal risk. Whitty (2018) opined that cybercrime offenders who are involved in the form of cybercrime that involve deep psychological harm and hurt to the victim (such as investment scam and romance scam) may have psychopathic tendencies. For example, someone who lacks empathy may be better at committing romance scam because they can dissociate themselves from the victim as they only see the crime as a business and their victims as preys. The first tenet of space transition theory (Jainshankar, 2008) explains this concept and it states that:

Persons with repressed criminal behaviour (in physical space) have a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space due to their status and position.

When an individual already lacks empathy or possesses psychopathic tendencies in physical space, they will find it easier to identify with the norms of the Yahoo-boy subculture because the cyberspace gives them the cloak of anonymity. Attractiveness and self-confidence are another feature that was identified by the study. They are very flashy people who like to show off their ill-gotten wealth. They are known to be very extravagant when they have parties or a reason to celebrate which could be a birthday celebration for both themselves and their girlfriends or just the success of a high paying scam.

In summary, the study found that individuals involved in cybercrime do not necessarily see their actions as being a crime, they see it as another form of work. This is an effort to neutralize their actions by not only reducing the consequences of their actions to just 'work', but they also separate themselves from their crimes by giving themselves nicknames. These nicknames are what they are called by, their friends are forbidden from calling them their legal names. In the cybercrime circle, work is referred to as 'ise' which is the Yoruba translation for work.

They can be identified with their flashy lifestyles which include expensive clothes, cars, mobile phones, wasteful and uncontrolled spending.

They are also known to hang out at night in groups and scarcely alone. Another major distinguishable features of a cybercrime offender in Nigeria are the hardened fingertips and lower palms. All of these are as result of the long hours spent on the computers. All the above characteristics are proven to be means of identifying cybercrime offenders in Nigeria. One might argue that many individuals possess these features and might not be cybercrime offenders. This is true, but it is too much of a coincidence for one individual to have all these traits both physical and psychological at once.

CONCLUSIONS AND RECOMMENDATIONS

The study examined the features of young cybercrime offenders in Lagos State, Nigeria, with a particular focus on their socio-demographic and psycho-demographic characteristics. The findings revealed that cybercrime in Nigeria is not a random occurrence but a socially organized activity with clear patterns of behavior, structure, and motivation. The majority of offenders are young, male, educated at least up to the secondary school level, and technologically inclined. They possess certain psycho-social traits such as the quest for quick wealth, lack of empathy, excessive materialism, manipulative tendencies, and a reliance on psychoactive substances. These characteristics not only distinguish them from their law-abiding peers but also explain their adaptability and persistence in cyberspace fraud.

The study underscores the theoretical relevance of Space Transition Theory, which aptly explains the behavioural shift that occurs when individuals move from physical space to cyberspace. In physical society, these offenders may conform to social norms, but the perceived anonymity and reduced risk of detection in the online environment encourage them to express repressed deviant tendencies. The cyberspace provides them with the illusion of impunity, enabling them to construct dual identities—one lawful and one deviant. This theoretical lens therefore helps to understand how young Nigerians rationalize their involvement in cybercrime as "hustle" rather than as criminality.

Furthermore, the findings suggest that socio-economic realities such as unemployment, peer influence, and weak moral institutions play a facilitating role in the development of the Yahoo-boy subculture. The glorification of wealth, especially within popular culture and social media, reinforces the notion that financial success—regardless of its source—earns respect in society. This has gradually normalized internet fraud among youths who see cybercrime as an accessible and rewarding career path, especially when compared to the limited opportunities in Nigeria's formal economy. The normalization of these acts, coupled with weak deterrent mechanisms and societal admiration for sudden wealth, perpetuates this deviant behaviour.

The psycho-demographic findings of the study also reveal the deep moral and psychological disconnect between offenders and their victims. The lack of empathy, as well as the tendency to dehumanize victims by calling them "maga" or "mugu," aligns with the denial of the victim technique in Sykes and Matza's (1957) theory of neutralization. This cognitive dissonance enables

offenders to justify their crimes and to frame cyber-fraud as a game rather than as exploitation. Similarly, the collective nature of the crime—manifested through organized roles such as catcher, picker, and sitter—illustrates the existence of an informal social organization that sustains and reinforces deviant norms.

From a policy perspective, the findings highlight an urgent need to strengthen preventive and corrective frameworks. Merely enforcing punitive laws without addressing the socio-economic and cultural roots of cybercrime will have limited effectiveness. There is also a growing necessity for public reorientation, especially among youths, to restore the values of honesty, diligence, and integrity.

In conclusion, combating cybercrime among Nigerian youths requires a multi-dimensional strategy; one that integrates sociological understanding, technological expertise, and moral education. The problem of cybercrime is not solely a function of individual deviance but a reflection of deeper societal contradictions, where moral decay, economic hardship, and technological opportunity intersect. Therefore, any meaningful intervention must address not only the symptoms but the root causes of the phenomenon. Only through sustained education, community engagement, and moral reform can Nigeria begin to reverse the tide of youth involvement in cybercrime.

1. Cyber Ethics and Digital Literacy in Education: There is a pressing need to incorporate digital ethics, responsible online behavior, and the legal implications of cybercrime into Nigeria's educational curriculum at all levels. Students should be taught not only computer skills but also moral responsibility in the digital age.
2. Value Reorientation Campaigns: The Nigerian government and civil society organizations should embark on value reorientation programs aimed at countering the glorification of cybercrime. Partnerships with musicians, actors, and social media influencers can help reshape youth perceptions about success and wealth.
3. Parental and Community Involvement: Parents should be more involved in the digital lives of their children by monitoring internet use, providing moral guidance, and discouraging unhealthy peer associations. Community-based mentorship programs can help redirect at-risk youths toward legitimate entrepreneurial ventures.
4. Enhanced Rehabilitation and Reintegration Programs: Correctional facilities should go beyond punitive measures to offer skill development, behavioral therapy, and counseling tailored to cyber offenders. Rehabilitation must include both digital and moral education to facilitate genuine reformation and reintegration into society.
5. Stronger Cyber Policing and Legal Framework: Nigeria's cybercrime units should be better equipped with forensic tools and trained personnel to match the sophistication of cyber offenders. The government should also ensure that laws against cybercrime are effectively enforced to serve as deterrents.

6. Addressing Youth Unemployment: Government agencies and private organizations should provide sustainable job opportunities and digital entrepreneurship programs to channel the talents of Nigerian youths into productive endeavors rather than illicit cyber activities.

FURTHER STUDY

Future studies should explore gender differences, the psychological profiles of offenders, and the transition from petty online scams to large-scale international cybercrime. Longitudinal studies can also help understand how changes in technology and society influence cybercrime patterns.

REFERENCES

Adeniran, A. I. (2008). The Internet and Emergence of Yahooboys sub-Culture in Nigeria. International Journal of Cyber Criminology, 2(2).

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Journal of Social Science Research, 6(1), 56–65.

Jaishankar, K. (2008). Space transition theory of cyber-crimes. Internet Journal of Criminology, 1(1), 1–11.

Katz, J., & Rice, R. (2003). Comparing internet and mobile phone usage. Social Science Quarterly, 84(2), 417–431.

Kukar-Kinney, M., Intihar, A. and Leahy, N. (2008). Negative Consequences of Internet Consumption: A Qualitative Survey. European Advances in Consumer Research. Vol. 8.

Lazarus, S. (2018). Cybercrime and the culture of quick wealth in Nigeria. African Journal of Criminology, 4(1), 45–63.

Oyenuga, A. (2017). Youth culture and cybercrime in Nigeria. Nigeria Journal of Criminology, 5(3), 23–41.

Sanou, B. (2017). ICT facts and figures. International Telecommunication Union (ITU) Report.

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. Cyber Psychology Review, 3(2), 1–14.

Whitty, M. (2018). The psychology of cyber offenders. Crime, Media, and Culture, 14(2), 259–278.